Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems

Ambili K N[1[0000-0002-8451-2497]] and Jimmy Jose[1[0000-0001-7074-090X]]

[1] National Institute of Technology Calicut, India
{ambili_p180002cs,jimmy}@nitc.ac.in

Abstract. IoT systems are vulnerable to various cyber attacks as they form a subset of the Internet. Insider attacks find more significance since many devices are configured to access the Internet without intrusion detection systems or firewalls in place. The current work focuses on three insider attacks, namely, blackhole attack, sinkhole attack and wormhole attack. A distributed trust based intrusion detection system is proposed to detect these attacks. The trust scores are compared with those existing in immutable distributed ledger and used to arrive at a decision to include or exclude a node.

Keywords: IoT, blackhole, sinkhole, wormhole, IDS,DDoS.

1 Introduction

Internet of things (IoT) finds special significance due to its application in everyday life. Several architectures have been put forward for IoT of which five-layered one [1] provides most abstract and clear topology. The five layers are business layer, application layer, service management or middleware (pairing) layer, object abstraction layer and object layer.

The business layer is a management layer which manages overall IoT system activities and services by building business models, graphs, etc. based on data received from application layer. The application layer provides services requested by customers.

Service management is a middleware layer that pairs a service with its requester based on addresses and names. This layer enables the IoT application programmers to work with heterogeneous objects across different hardware platforms. This layer processes received data and uses it arrive at decisions. The required services are delivered over the network wire protocols.

Object abstraction layer transfers data produced by the object layer to the service management layer through secure channels. Data can be transferred through various technologies such as RFID, WiFi, Bluetooth Low Energy (BLE), ZigBee, etc. The object layer involves the physical sensors of the IoT that aim to collect and process information. The sensors and actuators perform different functionalities like querying temperature, humidity, vibration, weight, etc.

The devices in IoT may be directly connected to the Internet or they can be connected through a gateway, forming a local area network which then connects to the Internet. The IoT environment is based on wireless or wired sensors and its applications.

The communication model based on clients and servers is applicable to IoT systems. Since most of the systems are triggered by signals from sensors or as response to actuators, publish-subscribe model is suitable. In this model, a publisher categorizes the messages to be published into classes using brokers. The subscribers can receive messages from brokers. A push-pull model may also be used. It uses queues. The messages are pushed into the queue by senders and pulled out by receivers.

2 Attacks in IoT

IoT inherits all the possible cyber attacks from the Internet. Due to the heterogeneity of devices involved and variety of protocols used at various layers by different vendors, multitude of cross-platform malwares are possible.

IoT security becomes complicated with interoperability issues and lack of uniform standards for technologies. Majority of the devices are made with intention of marketing quickly. Security by design has not been considered in the last few years of major releases. The devices have vulnerable interfaces. They do not provide options to update firmware on time. The IoT systems are accessible to various users over different networks. There is no strong system authentication in place to detect or prevent attacks like distributed denial of service (DDoS).

A comprehensive security analysis of IoT is provided in [2]. Another review paper on IoT security [3] outlined security requirements for IoT along with the existing attacks, threats and state of the art solutions. Network layer attacks include blackhole, sinkhole, wormhole attacks. Application layer attacks include web-based attacks, social engineering attack, buffer overflow, backdoor code attack, denial of service (DoS) attack. DoS attacks include flooding, reflection, amplification, jamming and DDoS attacks. Recent DDoS attacks (Mirai) have targeted smart grids as well.

Currently, the computers or laptops in various enterprises or organizations are managed by a network management system. Intrusion detection systems and firewalls are in place that protect these systems from external attacks. Insider attacks do not find much significance in closed network management environments.

A recent study on intrusion detection systems (IDS) [4] may be classifies them as rule-based or anomaly-based. Rule-based systems make use of known attacks to derive rules. Anomaly-based systems determine the abnormality in the system by analyzing data traffic. In [5], a mitigation strategy for blackhole attacks in mobile

ad hoc networks is described. A trust based intrusion detection system for wireless sensor networks is described in [6]. Distributed trust based intrusion detection approach which considers the interests of all participating nodes is discussed in [7]. Intrusion detection using a specification based system has been proposed in [8]. A trust based intrusion detection system specific to the routing layer protocol – routing protocol for low power and lossy network (RPL) - of IoT has been described in [9].

IoT systems bring Internet to our everyday life. This increases the risk of being target for various external attacks. Equally significant are insider attacks since many of these devices are easily available for purchase. These are passive attacks and do not require information about keys. An insider is in a position to extract key information if required as well. Here we consider three disastrous insider attacks, namely, blackhole, sinkhole and wormhole attack.

The sinkhole and blackhole attacks attract traffic by advertising a shorter route through the malicious node. In a sink hole attack, a group of malicious nodes send packets only to a particular sink node. A blackhole attack is a variation of sink hole attack wherein only one malicious sink node is present. The blackhole attack is also called packet dropping attack and first appeared in [10]. The packets are dropped by the blackhole node.

In a wormhole attack, two nodes which are at strategically important positions in the network decide to pair and analyze the network data. It is a passive attack. The attack is said to be in-band if tunnel is within the network and out-of-band if tunnel is formed outside the network. The out-of-band attacks are difficult to analyze and may leak out network data.

IDS should be lightweight. It is deployed at the gateway in centralized approach. In peer-to-peer IoT system, it is deployed on lightweight devices. The focus of this paper is on IDS for distributed IoT system for the three insider attacks mentioned above.

3 Trust based IDS solution

We propose an IDS based on trust. It takes into account trustworthiness of nodes. The trust score is calculated based on node behavior detected from responses to request queries. The trust score is stored in blockchain.

The initial trust scores are evaluated based on configuration details loaded into the device at the time of shipment. It is stored in the blockchain when the device enters the network. Each node behaves as a monitor node and evaluates the trust of all the neighbors that it interacts with. The trust score is calculated based on observed behavior of neighbor nodes.

The observed behavior uses honesty, lack of cooperation and reception of packets only from neighboring nodes to evaluate trust scores. Uncooperative behavior as an index can be used to detect malicious packet forwarding and dropping. Honesty as an index can help find blackhole nodes.

Every node in the network must maintain a neighborhood table which will consist of node ID of the neighbor nodes. A complete network is considered wherein the devices are permitted to communicate with one another.

The trust management system uses leader election in complete network as a method to arrive at trust that is to be stored into the distributed ledger. This is useful for mobile and stationary wireless IoT networks. The blockchain is managed by a consortium of network managers. The underlying assumption is that as time passes, nodes interact with more neighbors unless the system is getting destabilized.

Considering uncooperative behavior as an index by tracking the route of data, malicious packet forwarding and dropping can be detected. By using honesty as parameter (packets in and packets out), blackhole attack can be detected. By observing deviation from normal routes, sinkhole or malicious nodes forwarding data to the sinkhole can be detected. An in-band wormhole attack is detected when a packet not belonging to any of the neighbors, as per neighborhood table, is received. Out-of-band wormholes are difficult to detect since searching for such scenario leads us beyond the network under study.

Each node participating in the process is a monitor node and prepares a transaction record. This is sent across to all neighbor nodes in specific intervals of time.

Figure 1 : Transaction record

PIPO	Two dimensional
Route	List
Unknown Sender	Count

It has following three fields as shown in figure (1):

PIPO – a two dimensional vector with neighbor node value and difference of packets in and packets out (PIPO)

Route – list of unique routes in the packets it received

Unknown sender – count of packets received from unknown senders (those not present in its neighbor table)

The node which has highest trust score, as per the latest information in the blockchain, is chosen as the leader. The below pseudo code captures the details of functionality of leader node.

Input **:** transaction record of all participating nodes
Output **:** alert message, new trust scores
Pseudo code **:**
Repeat until a new trust score higher than self score is obtained:

a) Gather the transaction details of all member nodes.
b) PIPO values of communicating nodes is compared. If equal, increment trust score of both the nodes, else do nothing
c) Compare the list of unique routes and check if any route other than the one permitted by routing protocol appears. If yes, decrement the trust score of all nodes from the point at which discrepancy occurs, else do nothing
d) If unknown sender count is greater than zero, check the routes to see if nodes not permitted as per the routing table appears. If yes, decrement the trust score of the just preceding node.
e) If the evaluated trust score of a node is less than that in the latest block of blockchain, raise an alert message to participating nodes except the cur rently evaluated node of an intrusion detection.
f) Include new trust scores record to blockchain.
g) Initialize trust score of each participating node to last trust score from ledger.

A new leader node starts functioning when a node with higher trust score than that of current leader appears in the system. The current leader needs to inform this change to all nodes. Also, analytics on the trust details of a node, as saved in the blockchain, give good insights into trustworthiness of a node through blockchain analytics.

4 Conclusion and future work

Intrusion detection system based on trust score evaluated in a distributed way make infringement difficult. Attempts to evade IDS is not possible since IDS uses history from blockchain to validate the trust scores. A transaction with manipulated trust score is not acceptable. However, 51% attack in proof-of-work based consensus wherein majority takes control of adding blocks to the blockchain is possible. Other attacks due to the drawback of consensus method also prevails. In current work, we have not considered out-of-band wormhole as it leads beyond the net-work.

References

1. A.Al-Fuqaha, M. Guizani, M Mohammadi, M. Aledhari, M. Ayyash: Internet of things: a survey on enabling technologies, protocols and applications, IEEE Communications Surveys & Tutorials 17(4), 2347-2376 (2015)

2. Panagiotis I. Radoglou Grammatikis, Panagiotis G. Sarigiannidis, Ioannis D. Moscholios: Securing the Internet of Things: Challenges, threats and solutions, Elsevier Internet of Things, Volume 5, pp.41-70, (2019)

3. Mohab Aly, Foutse Khomh, Mohamed Haoues, Alejandro Quintero, Soumaya Yacout, Enforcing security in Internet of Things frameworks: A systematic literature review, Internet of things, Elsevier Volume 6 (2019)

4. Bruno Bogas Zarpelao, Rodrigo Sanches Miani, Claudio Toshio Kawakani, Sean arlisto de Alvarenga, A survey of intrusion detection in Internet of Things, Journal of Network and Computer Applications, Volume 84 (2017)

5. Ming-Yang Su, Kun-Lin Chiang, Wei-Cheng Liao, Mitigation of black hole nodes in MANET, International Symposium on Parallel and distributed processing with applications, Taipei (2010)

6. Fenye Bao, Ing-Ray Chen, MoonJeong Chang, Jin-Hee Cho, Trust-Based Intrusion Detection in Wireless Sensor Networks, IEEE International Conference on Communications, IEEE, Kyoto (2011)

7. Amol R. Dhakne, Dr. P.N. Chatur, Distributed Trust based Intrusion Detection Approach in Wireless Sensor Network, Communication, Control and Intelligent Systems IEEE, Mathura, India (2015)

8. Anhtuan Le, Jonathan Loo, Yuan Luo, Aboubaker Lasebae, Specification- based IDS for securing RPL from topology attacks, IFIP Wireless Days (WD), IEEE, Niagara Falls, Ontario, Canada (2011)

9. Faiza Medjek, Djamel Tandjaoui, Imed Romdhani, Nabil Djedjig,A trust based intrusion detection system for mobile RPL based networks, IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data, IEEE, Exeter, (2017)

10. Xiaobing Zhang, S.F. Wu, Zhi Fu, Tsung-Li Wu, Malicious packet dropping: how it might impact the TCP performance and how we can detect it, IEEE Proceedings 2000 International Conference on Network Protocols, IEEE, Osaka, Japan (2000)